Co-Designing for Community Oversight: Helping People Make Privacy and Security Decisions Together

CHHAYA CHOUHAN, University of Central Florida, USA
CHRISTY M. LAPERRIERE, University of Central Florida, USA
ZAINA ALJALLAD, University of Central Florida, USA
JESS KROPCZYNSKI, University of Cincinnati, USA
HEATHER LIPFORD, University of North Caroline Charlotte, USA
PAMELA J. WISNIEWSKI, University of Central Florida, USA

Collective feedback can support an individual's decision-making process. For instance, individuals often seek the advice of friends, family, and co-workers to help them make privacy decisions. However, current technologies often do not provide mechanisms for this type of collaborative interaction. To address this gap, we propose a novel model of Community Oversight for Privacy and Security ("CO-oPS"), which identifies mechanisms for users to interact with people they trust to help one another make digital privacy and security decisions. We apply our CO-oPS model in the context of mobile applications ("apps"). To interrogate and refine this model, we conducted participatory design sessions with 32 participants in small groups of 2-4 people who know one another, with the goal of designing a mobile app that facilitates collaborative privacy and security decision-making. We describe and reflect on the opportunities and challenges that arise from the unequal motivation and trust in seeking support and giving support within and beyond a community. Through this research, we contribute a novel framework for collaborative digital privacy and security decision-making and provide empirical evidence towards how researchers and designers might translate this framework into design-based features.

CCS Concepts: • **Human-centered computing** → Empirical studies in collaborative and social computing • **Security and privacy** → Social aspects of security and privacy

KEYWORDS: Community; mobile privacy; security; oversight; collaborative privacy; collective feedback

ACM Reference format:

Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, Pamela J. Wisniewski. Co-Designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3, CSCW, Article 146 (November 2019), 31 pages, https://doi.org/10.1145/3359248

1 INTRODUCTION

Many technology users learn about digital security and privacy from informal sources, such as stories from individuals they know [58]. Others report feeling uncertain and overwhelmed about how to manage their digital privacy and security to the point that they outsource these decisions to more knowledgeable users, such as their family members [24,28]. In many cases, when people

Author's addresses: C. Chouhan, Dept. of Computer Science, University of Central Florida, Orlando, USA; C. LaPerriere, Dept. of Computer Science, University of Central Florida, Orlando, USA; Z. Aljallad , Dept. of Computer Science, University of Central Florida, Orlando, USA; J. Kropczynski Dept. of Information Technology, University of Cincinnati, Cincinnati, USA; H. Lipford, Dept. of Computing and Informatics, University of North Carolina Charlotte, Charlotte, USA; P. Wisniewski, Dept. of Computer Science, University of Central Florida, Orlando, USA.

are in new situations or face uncertainty, they observe others and act similarly, or they ask friends or loved ones for advice. In turn, they provide guidance to friends and family members, those they work with, and to other individuals within their social networks [1,17,41].

In summary, users rely on their existing communities to help them make digital privacy and security choices. But seldom are these community-based social processes supported by technology. As a result, the information flows that aid individuals' privacy and security management within their socially constructed networks remain largely disconnected from design. Most technology solutions have not embedded mechanisms that afford the level of transparency and awareness needed to facilitate group-level privacy and security management within digital contexts.

To address this gap, we first propose a model of community oversight with mechanisms that support individuals' digital privacy and security practices. These mechanisms include increased transparency and awareness that allows trusted members of a community to provide relevant information, feedback, and assistance to help one another navigate the complexities of managing their digital privacy and security. Our model of community oversight is built on concepts drawn from the literature on citizen participation, community organizing, and proactive measures against risk. However, it is unclear how these concepts can be translated into design. We used a community-based participatory design approach to interrogate and improve our model of community oversight by noting mechanisms that participants used in the co-design of an app intended for community oversight, examining the following research questions:

RQ1: How can we translate users' needs for transparency, awareness, and individual participation into features that support the mechanisms of community oversight?

RQ2: Specifically, what features would people find useful in a mobile app designed to help them co-manage their digital privacy and security of their smartphones with others?

RQ3: What are the potential opportunities and challenges that emerge from this process of translating community oversight into interaction design patterns?

To answer these questions, we conducted Participatory Design (PD) sessions with 32 participants working in 13 small groups (of 2-4 members) for which they had existing relationships (e.g., friends, family members, and co-workers). We interviewed participants in their small groups and gave them a scenario-based task where they were asked to co-design new features for a mobile app for community oversight. We qualitatively examined the features based on how participants envisioned features would help them collaborate with their community members to make mobile app privacy and security decisions. This examination was then translated into the concepts in our model of community oversight. Overall, we found that users were concerned about online risks and would appreciate guidance not just from their community but also from strangers. Yet, while participants were comfortable with sharing their experiences and decisions within their community, many were less interested in performing direct oversight of others. Through this research, we make the following novel contributions:

- A novel model of community oversight based on the concepts of transparency, awareness, individual participation, and community.
- Empirical results from participatory design sessions that serve to translate these mechanisms into design-based features that people find useful for co-managing their mobile privacy and security.

- A revised model of community oversight based on the empirical study that incorporates the critical role of trust between community members and differentiates between active and passive individual participation.
- Design-based recommendations promoting collaboration among community members as it relates to digital privacy and security.

Thus, our research makes both theoretical and design-based contributions through the combination of our proposed model of community oversight and participatory design results.

2 RELEVANT BACKGROUND LITERATURE

Our research addresses the challenge of helping users collectively manage their digital privacy and security through the help of others. We first discuss research from the usable privacy and security community related to this goal, as well as research on mobile application privacy more generally. We will also discuss a broad range of motivating work on collective and social decision making when presenting our model in the following section.

2.1 Usable Privacy and Security Beyond the Individual

Much of the research in the usable security and privacy community has examined methods to better inform an individual's security and privacy practices, such as through improving interface designs to aid user understanding, and nudging users to consider the implications of their decisions more carefully [70]. While there has been considerably less focus on social processes, prior research has demonstrated the importance and prevalence of social processes in digital security and privacy management. For example, Pierce et al. [55] found that most cybersecurity toolkits focus more individual user's needs over community and that designers and researchers should develop tools that better support collective action. Rader et al. [57,58] examined how people learn about security advice and found that one important avenue is through the informal stories of security experiences told between friends and family. Indeed, family and peers are one of the most frequently used sources of security advice [59]. Dourish et al. [24] found that one common security management strategy was delegating security decisions to those more capable or interested, such as family members, knowledgeable colleagues, or roommates. Das et al. [19] conducted a study on mobile authentication for apps and found that individuals often warn their friends and loved ones to be careful after experiencing a security breach, reading about a security threat on the news, or observing a friend's insecure behavior. As such, Das and his colleagues affirm that social processes, such as social influence, do play a major role in security and privacy decisions, as social triggers can raise awareness, motivation, and knowledge about security [20]. Through a study of the adoption of security mechanisms on Facebook, they further demonstrated that the transparency of security features is critical to enable such social processes to occur [19,20]. They also found that people were more likely to adopt a security feature if a friend recommended it.

This prior literature shows that social processes can help people become more aware of issues surrounding digital privacy and security and influence behavior. However, few of these social processes have been explicitly reflected within technology mechanisms themselves. One exception is social navigation, providing interface cues regarding the decisions of other people, such as how many other users chose to share particular content. DiGioia and Dourish were the first to propose a social navigation mechanism to increase the transparency of privacy decisions by providing users with feedback on which files others made public in a peer to peer file sharing service [21].

Evaluations of this and similar mechanisms for cookies, instant messaging, and Facebook [6,33,54], demonstrated that cues derived from the privacy settings of others can influence one's choices. Social navigation mechanisms enable social comparison, allowing an individual to compare their decision against the social norms of other users. However, in all these cases, information flow is unidirectional, gathered and aggregated from a collection of other users and provided to the individual making a new decision. While Das et al. suggest that the observability provided by such mechanisms is best used to facilitate social learning conversations regarding others' behavior change [20], social navigation and similar mechanisms that have been proposed lack this support [43]. Therefore, we propose to examine the more influential process of oversight and understand the factors and challenges involved in providing oversight, to more explicitly help people help each other to manage security and privacy.

2.2 Security and Privacy in the Context of Mobile Applications

Smartphone use has become ubiquitous with 81% of adults in the U.S. owning a smartphone and 96% of those aged 18-29 being smartphone owners [75]. Mobile apps often require access to sensitive data (e.g., account, GPS, camera, and microphone) and services located in the cloud (e.g., Google, Facebook) to function properly [32]. As such, smartphone users share significant amounts of personal information through apps to third parties and other people [18]. This increases concerns about mobile privacy and security threats, such as malware, spyware, phishing attacks, and stolen or lost phones [76].

Several researchers have examined users' perceptions and mental models of mobile app privacy and security. For instance, Kelley et al. [39] founded that Android users do not understand app permission notification screens and are not aware of the potential security risks of accepting various app permissions. Shklovski et al. [60] studied users' attitudes towards data leakages. They found that users felt that these mobile apps violated their personal privacy in "creepy" ways but did very little to change their mobile app privacy behaviors based on this new information. To mitigate users' privacy concerns and increase awareness on how third-party applications can misuse private data, several technology-based solutions tools have been proposed, which can detect data leaks. For example, Gilbert et al. [32] developed AppInspector, an automated security validation system that analyzes apps and generates reports of potential security and privacy violations. Zhu et al. [74] built App Recommender, which automatically detects and evaluates the security risks of mobile apps to recommend safe apps. Others proposed security extensions such as MockDroid [5], and ProtectMyPrivacy [2], which replaces user's personal data with pseudo-data to protect the users' privacy.

An overarching theme of this research is to help individual users see how apps are using their data more transparently in hope of changing their behavior. Yet, Chin et al. [13] found that smartphone users were more likely to pay attention to social cues, such as reviews and ratings from other users than privacy indicators about android permissions. As such, we examine whether and how community oversight can be leveraged for mobile privacy and security.

2.3 Moving towards a Community-based Approach to Digital Privacy and Security

There are many examples that demonstrate how community oversight strengthens security and safety in the physical world – from parents watching over each other's children on the playground to neighbors alerting one another when a strange vehicle is near a home at an odd time. For instance, based on the premise of informal social control and social comparison theories,

neighborhood watches help enforce community-based standards as individuals participate in group activities to both accomplish group tasks (e.g., crime prevention), as well as evaluate and validate their own behaviors (e.g., protective measures) associated with the task at hand [27,60]. For example, neighborhood watches have been found to effectively reduce crime directly through "observe and report" mechanisms as well as by encouraging crime prevention practices among community members [29].

Public health is another domain in which community-based approaches have been embraced by researchers for deeply understanding factors that shape individual behaviors and lead to broader health outcomes within a community [38]. As a result, health behavior modification interventions often take an ecological approach where social and environmental factors are examined, as well as individual determinants of health [46]. Health-related systems have also followed suit – leveraging social media [40], social support [44], collaborative goal setting [14], and impression management [15] as persuasive tactics for helping people be healthier by making them accountable to others. Similarly, the key to the development of our mechanism of community oversight is to enable the collective capacity of a community of users to take simple actions to manage digital risks through raising awareness, motivation, and knowledge of privacy and security risks and behaviors. For example, a community could provide feedback to each other on which apps are the most private, which permissions make sense to allow, and whether any apps appear suspicious. By sharing this information beyond the individual, we may be able to influence the privacy behaviors of an entire community.

However, even within these contexts (e.g., neighborhoods and health), researchers have uncovered challenges to effectively deploying community oversight models. For instance, Purenne and Palierse [56] found that community-based surveillance programs implemented in France and Canada instilled fear and increased suspicion among community members. Others have found that while neighborhood watch programs seem to help reduce crime rates, they are less effective in crime-ridden areas [66], less successful in heterogeneous neighborhoods [60], and tend to promote racism [42]. In public health contexts different challenges arose, McNeill et al. [48] found that elderly people were often hesitant to share their health information within their social network and only a few studies have shown significant behavioral changes over a long period of time [49,68]. Therefore, while previous literature shows promise in community-based approaches for helping people manage risks, this warrants a deeper examination on how such a framework could be applied to digital privacy and security.

3 A MODEL OF COMMUNITY OVERSIGHT

According to Habermas, discussion among individuals is instrumental in the identification of societal problems and resulting collective action to resolve these issues [34]. Meanwhile, much of the decision-making about mobile app privacy and security is left to smart phone users to handle individually. We believe that community-level awareness can help to identify problems and support shared knowledge of possible solutions. Thus, our model of community oversight draws upon broader research from the social sciences, including citizen participation in problem-solving, community organizing, and proactive or preventative measures against risk [29,36,62–64]. Previous research has engaged citizens to monitor their local communities through transparency [6,7], awareness [11,35,71], and participation in solution-oriented discussions about issues impacting the community [12,71].

We have utilized this related work to form the basis for our community oversight model in the domain of digital privacy and security (Figure 1). Utilizing these concepts, we aim to use

sociotechnical design to increase the collective capacity of groups to address challenges that are external to that group.

3.1 Community

Our model of community oversight extends prior research that shows people often have established interpersonal relationships in which they already informally discuss their digital privacy and security [57,58], and this informal feedback could be enhanced through technical support. Communities define membership by shared attributes of people in it, the strength of their connections, or geographically bounded areas [11,12]. There are a variety of potential communities where oversight can occur, such as within organizations [43], families [16], a user's online social network [43], or even community groups [63]. A challenge to collective activities is that members of communities are divided by age, gender, or interest area preventing consistent communication and common understanding within the community [37].

The structure and nature of the relationships within groups, such as the level of trust between group members, as well as the shared purpose of the group, will impact the rest of the model. For example, community oversight mechanisms may not be well suited for groups where participants are suspicious of one another; as such, models assume a degree of trust and mutual interest among participants [29]. As such, a question we begin to investigate in this paper is what types of communities are interested and willing to collaborate around mobile privacy and security decisions. As discussed in the next sections, this community-based model leverages transparency and awareness as mechanisms to increase individual participation necessary to support community oversight for digital privacy and security.

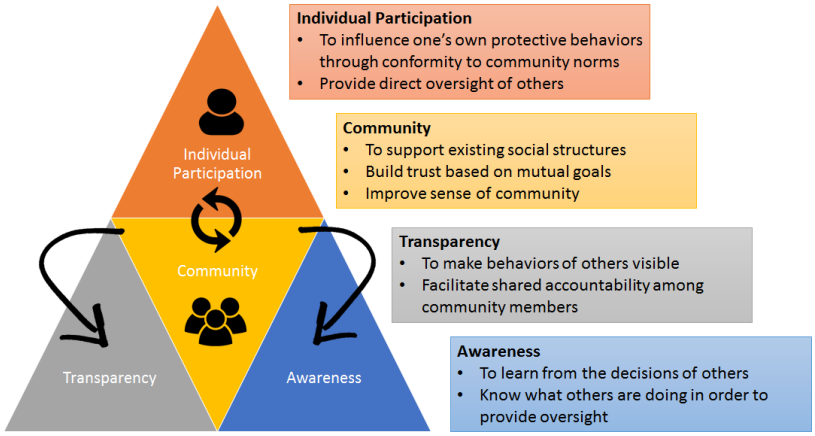

Fig. 1. Proposed Model of Community Oversight

3.2 Transparency

As Das et al. demonstrate, social processes cannot occur if users cannot determine what other people are doing [20]. Similarly, transparency of group members' privacy and security practices is a requirement of community oversight. We operationalize transparency here as the act of making this information available, however, there is no guarantee that available information will meet users' information needs [7]. An important research question that follows is what kinds of practices are potentially useful for other users to know about or provide feedback on.

Paradoxically, a key concern with increasing the transparency of an individual's privacy and security practices is privacy. Users must be comfortable sharing this information with other group members, and such transparency should not compromise their own security and privacy goals. We examine users' perceptions and concerns with transparently sharing their mobile app settings and actions, as well as the necessary features within a mechanism that enable users to control that transparency.

3.3 Awareness

We view transparency as a prerequisite to creating an awareness of information with which users can engage. In other words, community oversight depends not just on making information about the security and privacy practices of others available, but also presenting that information in such a way that group members can understand and engage with it. Situational awareness is understanding what is going on around you and using that understanding to make better decisions [25]. Tools that leverage community awareness allow individuals to engage with transparent information about their community in a way that connects users to their own information needs and serves as a basis for their own behaviors [11,35,71]. Prior work within the computing community to support social influence processes have focused primarily on social comparison – being aware of the community norms regarding an action to inform one's own behavior through crowdsourcing and social navigation [21]. We go beyond prior work by extending this awareness to enable oversight and feedback between group members. Users must be notified and encouraged to engage with the information because group members are unlikely to seek out this information when security and privacy practices are only performed intermittently [29].

3.4 Individual Participation

Individual participation in a community oversight mechanism is two-fold. First, users can utilize the knowledge and feedback of others to inform their own individual decision making. Moreover, users will need to be encouraged to oversee and provide feedback on the actions of others. We acknowledge that this model may impose some level of burden on users to not only manage their own privacy and security practices, but also invest in the shared responsibility of helping community members. For example, in crime prevention contexts, individual participation may come in the form of direct oversight through a willingness for individuals within the community to enforce standards for appropriate behavior - "eyes and ears" [29]. Otherwise, participation can be more indirect, by actively encouraging enhanced security or protective behaviors among community members [29]. Similarly, technology-supported communication can take the form of direct conversations, as well as other lightweight interactions for providing feedback and guidance, such as liking or questioning others' settings or installations [12,71]. In this paper, we explore the technical affordances that potential users can envision utilizing for mobile security and privacy oversight.

4 METHODS

Our model of community oversight may be a useful mechanism within a variety of digital privacy and security domains (e.g., web, Internet of Things, mobile, etc.); however, we embed our study in the context of mobile security and privacy to provide the specific social context necessary for our participants/co-designers to concretely think about privacy and provide feedback. We describe our participatory design sessions in more detail below.

4.1 Participatory Design Sessions

Participatory design (PD) is a technique where designers (or researchers) work with potential end-users of a system to co-create features that meet users' needs [52,67]. Muller and Druin [51] described participatory design as a "third space in HCI," somewhere between the users' domain and that of the technology developers' domain. In this space, users can challenge our underlying assumptions, generate new ideas, and co-create better design solutions than we would have envisioned on our own. PD gives researchers a unique opportunity to interrogate their own ideas (in this case, our proposed model of community oversight) and, more importantly, to take a generative approach to extend beyond their preconceptions [51]. While PD is often done with individual users, DiSalvo et al. [23] introduced the idea of community-based participatory design, in which PD is used *with* the help of community members, *by* communities themselves, and *for* the use of communities. DiSalvo applied this method to co-creation of technology-based solutions in community settings, such as neighborhoods [22]. Mir et al. [50] extended this community-based PD approach to the context of privacy policy design for marginalized populations. They proposed directly engaging with communities (e.g., people with HIV) to understand contextual norms around information sharing to better inform privacy policies. In our case, we are designing *with* and *for* the community, but have not limited the scope of our community to a specific common attribute or to physical neighborhoods of people within close proximity, as digital privacy and security is not confined to a specific segment of the population or one's physical location. Instead, we invited individuals interested in privacy and security to self-identify community members that they would be comfortable sharing privacy and security decision-making with and ask them to engage in sessions to co-design of an app to be used by other communities with similar interests.

Muller and Druin [51] describe a diversity of techniques and methods to engage participants in PD. One such method is PD "workshops" where groups of interested parties and stakeholders to introduce novel procedures through a process of: "Critiquing the present; Envisioning the future; Implementing – moving from the present to the future. (p.20)" Our approach follows from this method by engaging small groups in a process of first understanding a present problem through the introduction of a problem scenario. This adaptation of the critiquing phase supports collaborative problem solving for a common privacy and security issue without requiring participants to be conversationally familiar with many privacy concerns in advance of participation. Next, small groups work to co-design (and redesign) a envisions solution to this problem, and finally, they present their design as it would be implemented within their community. Given the small group size (2-4 participants) and relatively short length of time (90 minutes) we adopt the term "PD sessions" rather than workshops.

This approach is well-suited for this study because: 1) we intended on designing for communities with the help of these communities, 2) we did not want to constrain our design with our own preconceived notions of community oversight, and 3) it allowed us to observe how mechanisms in our model were translated into design by communities. While we propose our model as a starting point, our goal in choosing community-based PD as our methodological approach was to first understand how community oversight can help them manage their privacy; second, how they would design a technology intended to support community oversight and third, to gain empirical insights directly from our participants on what we got right, what we got wrong, and what we missed in our theoretical model. We also did not introduce our model to our participants so as to not influence our participant's ideas rather we asked them to design an app which supports community collaboration to manage privacy and security. This PD session helped us understand how participants designed features that connected to our theoretical model as well

as how we can further improve our model. We describe our PD session design in the sections below:

4.1.1 Background Context: We started by asking participants questions related to how they currently manage their mobile app privacy. We included these questions to get a picture of how participants decided what permissions they would grant to mobile apps installed on their phone. To introduce the community aspect to our study, we asked small groups of participants if they discuss these issues with others before making mobile app privacy decisions.

4.1.2 Problem Scenario: Next, we took inspiration from past research which used scenario-based approaches as an effective way of conducting participatory design [61,73]. We used storyboards to help participants visualize the problem of mobile app privacy breaches [4]. Our scenario was based on a mobile app called "Movie Pass," which was recently in the news for tracking users' locations at all times (Figure 2).

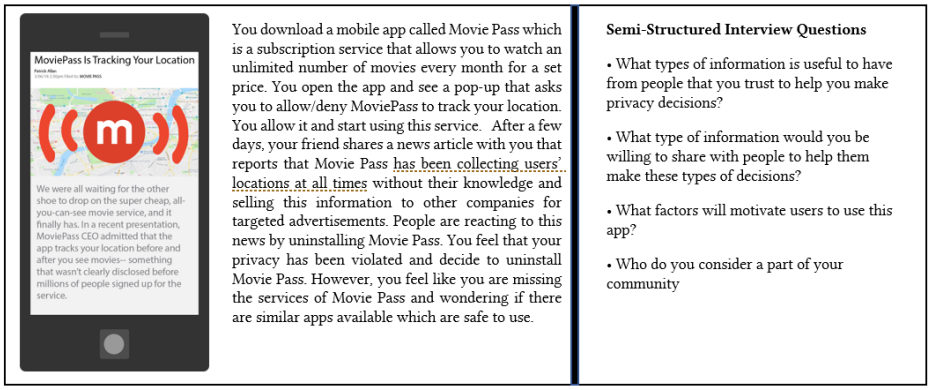

Fig. 2. Problem Scenario (left), Design Prompts (right)

4.1.3 Open Co-Design Session: After being introduced to the problem scenario, we asked participants to, "Design an app to help people manage their phone permissions and settings as a community." Participants were given large sheets of paper in which to draw their app design (Figure 3). We used the "Bags of Stuff" technique, a low-tech prototyping approach, where participants are given generic design elements, such as a message bubble, like buttons, dislike buttons, on/off toggles, and alert notifications, to overcome the "fear of drawing" [51]. We provided an "element directory," which defined each of these elements. For example, "Like" was described as a button that allows the user to express that they like, enjoy, or support certain content. We explicitly told participants they were not required to use any of these elements in their designs. The only interactions the researchers had with participants during this part of the session was to ask them the design prompt questions shown in Figure 2.

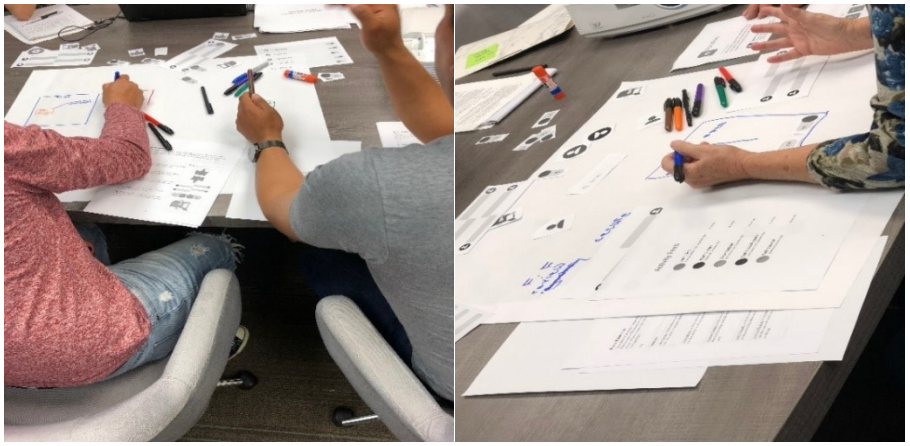

Fig. 3 Participatory Design Session. Open Co-Design Session (Left) and Feature Introduction/Redesign (Right)

4.1.4 Feature Introduction and Redesign: Next, we wanted participants to iterate on their designs. We also introduced some pre-defined features that were created during a summer REU program [Anonymized for Review] to get feedback on them. These included an "Activity Feed," "Discover Page," and "Expert Users" (Figure 4). We again provided a directory and bag of stuff for these features similar to what we gave participants in the open co-design session. Participants were explicitly told that the use of these features was optional and that they could choose to use, modify, or discard any or all the features presented. The idea behind implementing this phase of the design process and providing these features was to elicit feedback from participants in order to help generate additional design ideas through their fresh perspective and feedback. This redesign session was allotted approximately 20 minutes.

4.1.5 Presentation: After the redesign session was completed, we asked participants to present their final designs and walk through the functionality of each feature they incorporated in their designs taking note of how they related to mechanisms in our model (community, transparency, awareness, and individual participation). After the presentation, we collected demographic information and revisited some of the question we asked earlier. At the end of the session, we answered any questions participants may have had. Participants were then thanked for their time and were given a $15 Amazon gift card as compensation. On average, the study sessions lasted about 90 minutes.

4.2 Participant Recruitment and Profiles

We recruited participants through flyers, emails, and by word-of-mouth in the local vicinity of a large Southeastern public university in the United States. We stated in our recruitment materials that we were looking for "a community of two or three people who are comfortable sharing privacy decisions with one another." This included children who were accompanied by a parent or legal guardian. We intentionally left the definition of community open as we wanted to understand from participants how they envisioned their communities. We specifically reached out to different community organizations, such as schools, work offices, and elder communities to get diverse groups of people. We saw that most of our participants came with either family, friends, co-workers.

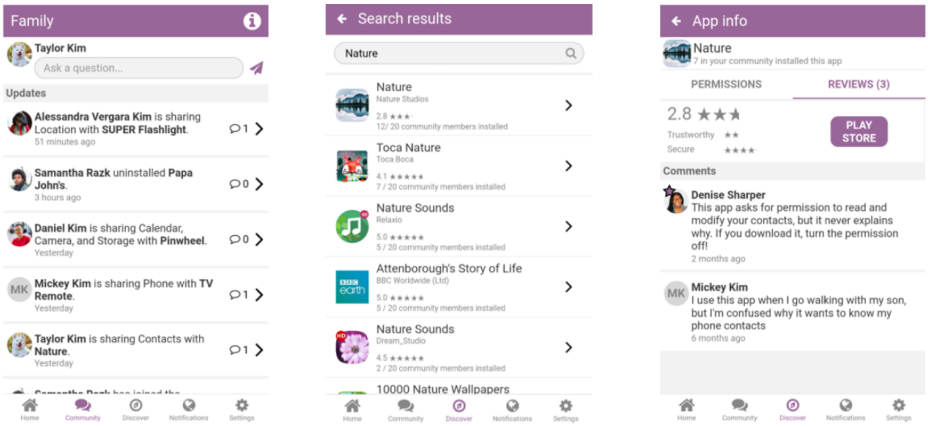

Fig. 4. Activity Feed (left), Discover (middle) and Expert User (right)

Prior to recruiting participants, the Institutional Review Boards (IRB) of the primary university conducting the study approved the study. On the day of the study, adults completed the informed consent process, and child participants (those under the age of 18) also provided their assent to participate. We recruited a total of 32 participants in small groups of 2-4 individuals at a time (13 groups in total) in which 15 identified as females and 17 as males with their ages ranging from 10 to 80 years (average age ~36 years) as shown in Table 1. There were 11 participants who identified as Caucasian, 10 as Hispanics, 5 as Middle Eastern, 4 as African American, and one as Asian. All the participants in a group owned and used a smartphone (iPhone and Android). Out of 13 groups, 7 were family, 2 were co-workers, 3 were friends, and one was a mixture family and friends. Several families also included children (less than 18 years of age) and in total 4 children participated with their parent(s).

Table 1. Participants' Demographic Information

Group	Group Type	Participant IDs	Groups Demographics (Relationship, Age, Gender)
1	Family	P1, P2, P3	Father (59, M), Daughter (18, F), Son (10, M)
2	Friends	P4, P5	Friend (27, F), Friend (29, F)
3	Family	P6, P7, P8	Father (45, M), Daughter (13, F), Daughter (15, F)
4	Friends	P9, P10	Friend (23, M), Friend (22, M)
5	Co-Workers	P11, P12	Co-Worker (39, F), Co-Worker (51, F)
6	Family	P13, P14	Wife (64, F), Husband (61, M)
7	Co-Workers	P15, P16	Co-Worker (44, F), Co-Worker (29, F)
8	Family	P17, P18, P19	Son (21, M), Daughter (16, F), Mother (52, F)
9	Family/Friends	P20, P21, P22	Husband (37, M), Wife (24, F), Friend (27, M)
10	Family	P23, P24	Wife (66, F), Husband (67, M)
11	Family	P25, P26	Brother (24, M), Brother (23, M)
12	Family	P27, P28	Wife (76, F), Husband (80, M)
13	Friends	P29, P30, P31, P32	Friend (23, M), Friend (23, M), Friend (23, M), Friend (23, M)

* M= Male, F= Female

4.3 Data Collection and Analysis Approach

4.3.1 Participatory Design Artifacts: The first three authors of this paper conducted all participatory design sessions together. Two forms of data were collected from the participatory design sessions: 1) video recordings of each session, and 2) the physical design artifacts. During the design sessions, a video camera was aimed at the table in which participants created their designs, as to avoid capturing their faces. After the session concluded, the three research team members discussed the session and created a debriefing document to record their thoughts about the session. Two of these team members transcribed the video recorded sessions verbatim, which were then qualitatively coded for insights. We took pictures of the design artifacts and included this imagery in our qualitative analyses. Each group and participant were assigned unique identifiers, which are used in the presentation of our results to maintain the confidentiality of our participants.

4.3.2 A Hybrid Data Analysis Approach: Our proposed model of community oversight served as a grounding framework for designing participatory design sessions to answer our high-level research questions. Specifically, we wanted to analyze the data using both inductive as well as deductive data analysis technique to understand how participants designed practical features that support collaborative privacy management (RQ1) in the context of a mobile apps (RQ2) that related to the concepts in our theoretical model. We were able to better understand how participants perceived and designed for community oversight as well as refine our model based on those designs. Further, we used an open-coding approach that allowed new themes to emerge from the participatory design sessions that shed light on the limitations of our model (RQ3). Therefore, a strength of this research is in our hybrid approach to combine theory (top-down) and empirical evidence (bottom-up) to test, refine and extend a model of community oversight for digital privacy and security.

To this end, we qualitatively coded our data using a hybrid approach of deductive (top-down) and inductive analyses (bottom-up) [26]. First, we template coded our data based on our theoretically driven model of community oversight. Specifically, we coded for: 1) how participants envisioned community, 2) the level of transparency they were comfortable with sharing information with others, and 3) the types of information they felt would be helpful to raise awareness about mobile app privacy and security concerns, and 4) how and whether they would individually participate in such a community. Second, we used a inductive approach to identify and conceptually group the unique features that would support community oversight that our participants created. This analysis included both the transcriptions and the design artifacts. Since there was some overlap between the features participants designed on their own during the open co-design session (section 4.1.3) versus the features we introduced in the redesign session (section 4.1.4), we discuss the distinction between these generative versus confirmatory findings in more depth in our results. Finally, we engaged in open coding of emerging themes. The two strongest emergent themes included 1) participants' need for trust among community members and the information provided from one's community, 2) and the lack of motivation to actively participate, which led for the need for passive participation through automation.

The three team members who conducted the participatory design sessions worked closely together to iteratively code the data and form a consensus among their codes. The remaining authors helped guide their analyses and interpretation of the results, as shown below.

5 RESULTS

We start by reflecting on what participants thought about various aspects of our model of community oversight based on their discussions throughout their design process. We then discuss the specific features they designed. We also discuss how these features tie back to our model and promote transparency, awareness, and individual participation.

5.1 User's Perspective on the Model of Community Oversight

5.1.1 Community: First, we wanted to see who participants considered a part of their community. While developing the model, we conceptualized communities as closed groups of people who felt comfortable discussing their mobile privacy and security with one another, like families, parent-teacher associations, church groups, elder communities, or people who work together at the same organization (co-workers). However, participants had a different perspective on the word community. Their first perspective on community was implicitly noted by observing with whom they chose to participate in the study. Over half (7) of the groups consisted of family members, while the rest were friends and co-workers. Their second perspective was noted when we asked them that, in the context of privacy and security, who would they consider their community. In this case participants went beyond this inner circle. In fact, 84% (27 out of 32) of our participants mentioned that they would appreciate help from anyone who uses the same app or even people they do not typically interact with who live within a certain physical range with them. Participants wanted to have this more public aspect of the app for very specific reasons. First, there was no way to guarantee that everyone in their inner circle would have the app for which they sought advice. Second, they were not sure if the expertise they needed existed within their more intimate social networks. Therefore, they felt that they needed some way to get this outside expertise. For example, P6, a father who participated in the study with his daughters, said that he himself would not know enough to advise anyone:

"Hmm if they thought they were being scammed or something I would say maybe you should not allow cookies or not cookies, but don't allow that or something. I don't know enough to really advise anyone." -P6

Having reviews from a larger population would provide them with more information from wider range of individuals to help them get more useful information. Participants said that while they may not always trust a stranger's advice, they would appreciate any help they could get. Therefore, while we envisioned this app to be a more private app (within a closed community), many participants thought the app should be more flexible, allowing them to connect with their trusted inner circle, but also benefiting from the expert advice of others outside of that circle. It was also interesting that some participants used physical proximity (even though the concept of neighborhood watches was never mentioned to our participants) as a way to define their community.

"Actually, I was thinking that you could have a local and global, because if no one in your areas has the app, then it's hard to say whether it is useful or not so if you have a global that might be a little more useful." -P25

However, participants were also clear that they would only be willing to help people within their inner circle with privacy and security decisions. For instance, 56% (N=18) of our participants said that they would be mostly concerned with helping their family members, as opposed to strangers. Among these participants, 16 participants said that they would use this app to keep track of what their children or grandchildren were doing, similar to parental control apps [31,72], to make sure they not exposing themselves to risks. Five groups (G3-Family, G7-Co-workers, G9-Family/Friends, G10-Family, G13-Friends) suggested features to track family members more

directly. In this sense, they wanted to have oversight over a particular individual, such as an older parent or a child. This oversight was designed to allow users to view the privacy decisions of those they wanted to more directly advise. In other words, oversight was not necessarily community-wide, but instead focused on care relationships.

We also noticed that participants designed differently depending on with whom they participated in the study. For example, groups of families designed the app particularly for helping their family members, whereas groups of coworkers and friends often designed for a broader range of scenarios, where a design feature that they might not see themselves using, they would keep it in case others might find it useful. This shows that participants were inclusive of the needs of others and wanted to guide them to keep the community safe overall.

5.1.2 Transparency: Participants had diverse views about transparency in terms of providing transparent information to community members, as well as receiving transparent information from them. We asked participants what information they would like to share with others in order to help them make privacy decisions. Nine groups said that they would share their personal experiences with the app by commenting on someone's activity or providing an app review about any issues they have faced or any security concerns they had. They also said that they would share their negative experiences but not necessarily positive ones.

"I would make the effort to go online and be like hey this is fraud, but if it's like, oh it's a good app, like some reviews I don't need honestly like when I go through reviews oh, it's a great app, elaborate like how" -P1

Others said that they did not feel comfortable in commenting; they would prefer to leave just star ratings.

"For me you like thumbs up or thumbs down, or I can do it just the rating, without having to leave a comment" -P5

Participants also mentioned that they would share which apps they have in their phones with their friends and family, so that others can see what permissions they have granted and learn from that to make their own decisions, but they would not share this information with others. However, they still wanted to have a level of privacy for that feature. Participants said that they would like an option of restricting certain apps from sharing with friends and family, such as private health apps, porn apps, or dating apps, which they do not want others to know about.

"P12: I would use that type of app on medical for myself or for my father who is elderly. I could enter something in regard to cancer for a family member or just out of curiosity, so I could have basic knowledge. Someone could see that and assume that I'm dealing with that or I'm suffering.

Researcher 1: And you would want that information to stay private?

P12: Right."

Participants also had a different perspective about sharing their personal information. Some participants were not comfortable with sharing reviews on the apps outside of their close community because they did not want their name to be public. For example, 21 participants desired to be able to post anonymously, explaining that users may be embarrassed of questions they were asking, or lack of motivation to create a profile. Among those, 10 participants were personally not comfortable sharing their names with strangers.

"Yeah, because sometimes there are posts and I want to respond to them, but I don't want my face to be attached to it. Because sometimes I have been through that and I want to respond, but because it's public I hate that. I would want something where users of the community can see this only or friends only can see my reply, you know." -P15

However, participants said that they would like to be anonymous only in the public part of the app; they were okay with having their name attached in their private groups like friends or family.

"The difference is that when it's a family member you would have no problem saying your opinions on the app, but if it's global or community wide I would prefer to do that anonymously." -P12

Overall, while participants desired transparency from strangers, they were reluctant to be transparent with their identity with others. Another interesting finding in the context of transparency was that participants wanted to be transparent only with the people they knew like their friends and family but not with strangers from whom they wanted external guidance. Although not related to our questions, participants often also mentioned wanting companies to be more transparent about how they were using their personal information, and this desire was seen in the features they designed.

5.1.3 Awareness: When asked about what information participants would like to see from their community members to help them make more informed decisions, all 32 participants said that they would like to read reviews about different apps provided by either their community members or strangers. Participants said that having reviews would save them time by not having to ask for the guidance in person and rather look it up on the app. Participants also said that having an option to see what permissions others in the community have granted to the apps they have in common would also help them decide.

"If it's a warning I would look into it, but if it's like an advertisement I won't necessarily trust it unless it's from someone I know." -P12

Participants also mentioned that while they do want information from their community members, they do not necessarily want regular updates about new app downloads or changes to permissions they are sharing. They would only look that up when they need that information (active vs passive). However, this attitude shifted among parents who wanted to provide oversight for their children by keeping track of what their children are doing.

"I mean I think this would have to be like a family plan or because you know, P4 is my friend but I don't want to be tracking what apps she downloaded, like I don't care. My son, yes I do care, maybe my mom or dad maybe they don't really know what's going on yes, but it would have to be very very private" -P5

Therefore, these were some of the ways, through which participants envisioned themselves using community information to become more aware of what others are doing. Along with this, participants also designed some automated features to help them make privacy decisions that we discuss in the Feature Analysis section.

5.1.4 Individual Participation: The model of community oversight depends on community members participating and helping one another. Most participants (24 out of 32) said that they would help others and guide/warn others by sharing their personal experiences. However, they would not be motivated to use the app just to help others. Their primary motivation was getting the information they needed when they needed it to make a privacy or security decision.

"I would use this app only if I was looking for information" -P9

Eight participants said that they would refrain from participating in the app through commenting more publicly and would only be willing to help their family members or friends. We also saw this hesitancy more among older participants who were not as educated on this topic and did not want to offer bad advice. Older participants indicated they were more inclined to read others' responses to help them make safer decisions online.

One of the themes that emerged was the concept of active versus passive participation. Participants did not want to help others at all time or wanted to be notified. They wanted to provide active oversight to their family only (sometime friends) while passive help to anyone else. To address passive help, participants designed various automated features that we discuss in the next section.

Overall, participants desired help from strangers but were less inclined to help strangers. Participants also wanted to know where their advice was coming from but were not willing to share their identities with strangers. Participants were willing to help their close community members, but acknowledged they were more motivated by receiving help than providing it. In addition, more active oversight and communication was desired only for those who already have such a relationship.

5.2 Translating Community Oversight into Community-based App Features

In this section, we describe the features designed by participants and how each feature set embodies different elements of community oversight. In Table 2, we conceptually grouped the different features that emerged from our participatory design session. We note when a feature was introduced by the researchers in the redesign phase (*) and whether participants suggested a similar feature (**) prior to our introducing the feature to them. Also, while most features had a community-based element, we included some features participants envisioned that were not community-oriented at the end of Table 2.

5.2.1 Expert Users: This was a feature presented by the researchers during the open co-design session, but five groups came up with a similar idea on their own. Overall, expert users were the most prominent design feature with all 13 groups incorporating this feature in their final designs. Expert user allowed for a sense of validation so that participants in the app could know when to trust or ignore certain advice. For those who saw this app as only consisting of friends and family, the expert user provided a way to fill the gaps when these small communities had no advice to give on particular apps or could not reach a consensus.

"Well maybe for that you could have something that you can tell them from everyone else and that they know what they are doing, like an expert. Something like not just a star, but maybe it looks a lot different so that people can easily notice it out of everyone else so that you know that they are experienced and know what they are doing so that they can leave a comment." -P8

Participants wanted these expert users to be as transparent as possible in order to receive the most accurate information. For instance, expert users would be identified with a blue verified check on their profile, similar to Instagram or Twitter which verify the authenticity of expert users. Participants also discussed who could become an expert user. Some suggestions included security experts, researchers, and people within the community that actively contributed high-quality information that other users found helpful.

Table 2. Feature Analysis

Feature Categories	Features	Description	Groups
Reviews & Ratings	Expert Users*	Qualified Users who have technical knowledge to advise others when community members lack technical expertise in providing guidance.	13 Groups (G1**, G2, G3, G4**, G5, G6, G7**, G8**, G9, G10**, G11, G12, G13)
	Discover*	A section of the app where individuals can search for apps and read reviews about them.	12 Groups (G1**, G2, G3**, G4**, G5**, G6**, G7, G8**, G9**, G10**, G11, G13*)
	Private/Public Feature	Public Feature – Reviews from everyone who uses the app or lives with certain distance (in addition to community members).	11 Groups (G1, G2, G3, G4, G5, G7, G8, G9, G10 G11, G13)
	Rating System	Individuals providing ratings for different apps as well as rating app reviews	5 Groups (G2, G5, G8, G11, G13)
Sharing Information Mechanisms	Sharing News Articles	Sharing news articles related to privacy and security within the community	6 Groups (G1, G5, G7, G10, G11, G13)
	Sharing Reviews	Sharing the reviews and feedback within community.	4 Groups (G5, G6, G7, G11)
Activity Awareness	Activity Feed*	A section of the app where individuals get auto-updates about certain activities from their community members.	4 Groups (G5, G6, G9, G11)
Non-Community Features	App Scanner	Scans the phone to assess if any apps are breaching the privacy permissions set up by the user. If a breach does occur, the app alerts the user.	11 Groups (G1, G2, G3, G4, G5, G6, G7, G8, G9, G10, G11)
	Simplified Privacy Agreements	A summary of app's privacy permissions in simple and easy to understand language which includes why the app is using certain resources	6 Groups (G1, G6, G7, G8, G9, G13)
	Privacy Alerts	Alerts when apps are accessing data, particularly location, in the background without user's knowledge	6 Groups (G2, G4, G7, G8, G9, G11)

**These design features were introduced to participants in the redesign session.*
***In these cases, participants came up with similar features on their own in the open co-design session.*

5.2.2 Discover: This feature was also designed by the research team; however, the majority of the groups (9 out of 13) designed a version of this feature even before it was presented to them. It is interesting to note that his feature's existence depends entirely upon a community-based model. The specific idea behind the design of this feature was that community members would provide reviews and ratings for different apps in order to learn from one another. Most participants saw that the reviews would include information such as what types of resources the app would ask for and which permissions were safe to accept and other information (shown in Figure 5, left). This information would provide a user with valuable data that they could use to make decisions about

whether they would like to download a particular app or if they would allow it to access specific information. Although this main premise was consistent amongst most of our groups, slight variations did occur, especially when this feature was presented during the redesign session. For instance, three groups were critical of the version presented by the research team, particularly, the "suggested for you and recommended for you" feature because they feared that getting recommendations would mean the app would invade their privacy. This perspective suggests that these participants were concerned about their privacy since they demonstrated that they were aware of how certain apps are able to access their personal data. The quote below demonstrates the desire for a feature such as the discover which relies upon group knowledge to make better individual decisions.

"Having something like this that I could go to would be amazing. To be able to get ratings, a score, but also to put out there the positives and negatives of a feature that companies themselves have researched and evidenced." -P11

Hence, through this feature participants envisioned themselves to look for right answers in their community before making a decision.

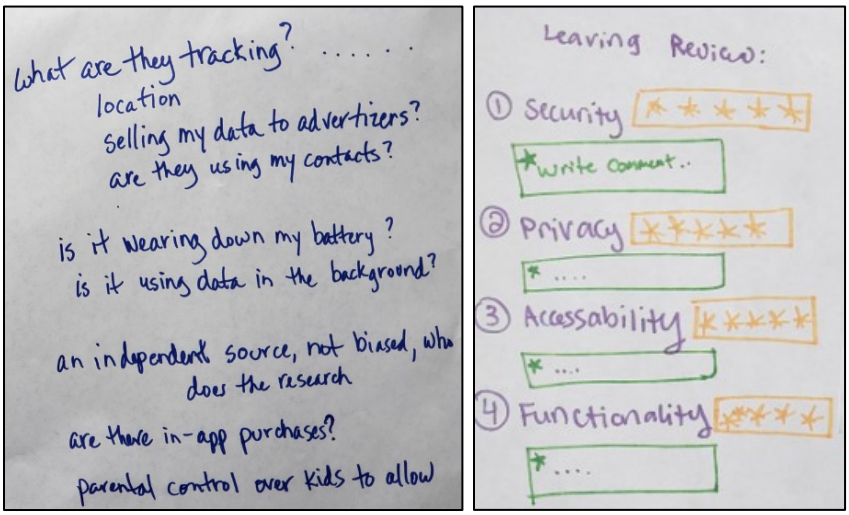

Fig. 5. Information Desired in the Reviews (Group 10) and Ratings (right, Group 2)

5.2.3 Private/Public Feature: Participants differed in who they saw as a best fit to provide ratings and reviews. As explained in section (5.1.1), some participants mentioned that they would appreciate advice from people outside their friends and family who use the same app. Therefore, 11 out of 13 groups wanted the app to have the option to get reviews from people outside their inner circle, while only two groups (G6, G12) wanted the reviews from only family and friends. One participant, P13, felt especially strong about this and said,

"A couple of years ago I would have said yes, but now I would say no because you've heard of Amazon and eBay having people being paid to write good reviews. So, for people like P14 and I that's why we rely on family and friends." -P13

Five groups saw that the best solution could be including both parts into the app so that they could have the option to access both public reviews as well as having a private group of friends and family members. In order to accommodate this, four groups proposed an option of filtering

the reviews. This filtering system would allow individuals to first see the advice of those whose opinion matters the most to them— whether that be community members, experts, or the general public.

5.2.4 Rating System: In addition, participants not only wanted to have information presented to them in a transparent manner, but also wanted a way to easily identify the types of information they should be looking for. Certain individuals felt as though they did not know where to look to determine which apps are safe or even what types of knowledge they should have about their mobile privacy and security. In order to address this, 5 groups designed a feature called a multi-factor rating system (Figure 5, right). People would rate the app based on its security, functionality, usability, privacy etc. Two groups designed a feature called Blacklist within which the reviews of community members could be highlighted and filtered into one place. For instance, if a certain percentage of the community's reviews were negative, apps would be added to this blacklist. These apps would then stand apart as those the community had voted to be especially dangerous and could most easily compromise a user's privacy. This list was designed as a way to highlight the apps that were viewed to be unreliable and unsafe and indicates participants' trust in community members to determine whether an app would appear on the blacklist. One participant spoke on this feature saying:

"I would like to create an app that I can go to find whether an app's been registered. I would like to know if others have used the app and whether it is safe or not." -P13

Many participants mentioned that they would rather provide rating than comment, hence rating system not only helps to get a picture of the privacy of the app but also helps to increase participation from wider range of individual.

5.2.5 Sharing Information Mechanisms: One of the ways through which participants thought of helping their community members as well as helping themselves was by sharing the reviews they read about certain apps through direct messaging or posting (G5, G6, G7, G11) as shown in Figure 6 (left). Such a feature helps to increase awareness more generally across the community. This feature was made for helping more intimate community (family, friends, co-workers) as compared to global community as participants were not highly motivated to help strangers. This feature would also provide a user with the explicit control to direct information to others when they feel it will be useful or helpful to another individual. Such an idea supports the notion of community participation as it provides a direct mechanism upon which users of this app can intervene in their community's decision-making processes. The difference between this feature and others is its private nature. Through more direct messaging, a user has the ability to control who sees what information and how they see it. It was brought up by a select number of participants that such an opportunity would allow them to participate more frequently in this app as it would support conversations in an easy manner about the topic of privacy and security.

Apart from being aware of how safe their phone is, they also wanted to keep up to date with what is currently happening in the field of security and six groups (G1, G5, G7, G10, G11, G13) came up with a new section called "News Article/Latest News" (Figure 6, right) which would feature the latest news articles or horror stories related to mobile app permissions and privacy violations. Participants designed this in order to motivate themselves and others to care more about their privacy. Participants also mentioned that there should be an option of sharing news articles with their community members using direct messaging to spread awareness in their community.

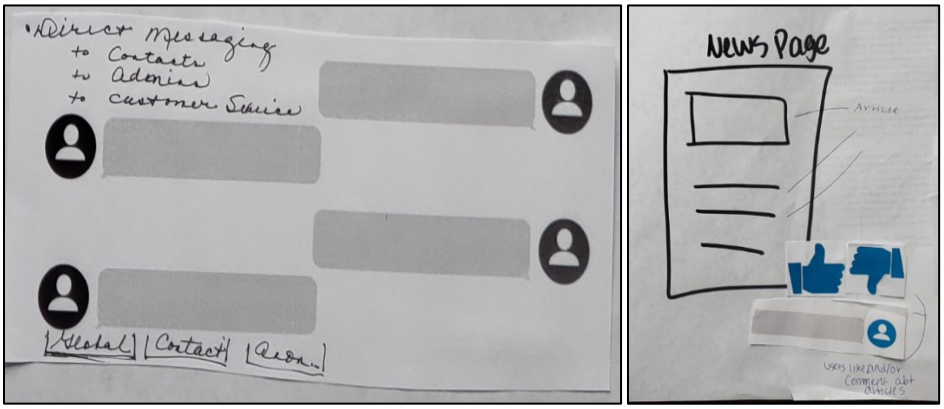

Fig. 6. Sharing Reviews via Direct Messaging (left, Group 5) and News Section (right, Group 2)

5.2.6 Activity Feed: One feature that reflected the idea of a tight-knit community group (family, friends, co-workers) was the activity feed. The activity feed was a feature we introduced during the redesign session, where users could see a feed of information from their closed community group. This feed would display information on how members of the community made privacy permission decisions and could then allow other members to advise/warn on these. None of the participants came up with a feature similar to the activity feed during the open co-design session, and only 4 out of the 13 user groups said they would use the activity feed after it was introduced in the redesign session. All the eight groups had a similar rationale: that they did not want to keep track of what others are doing and did not want others to keep track of what they are doing. They thought that this feature was both intrusive and contained information that would not necessarily lead to safer decisions.

"No, because for me like I honestly don't care what other people do. Like if I cared about a specific app I'd go to the app and see which people posted. I don't need to be constantly told this person commented on this or this person commented." -P4

Interestingly, the participants who liked this feature were mostly parents who wanted to keep track of what their children are doing. The auto-updates will help those parents to act in a timely manner whenever their children are making unsafe decisions while downloading mobile apps. However, groups differed on how they will help their children. P6, a father of two teenage girls said that he should have an option to control what his children are doing through this app (Figure 7, left). His daughter (age 13) supported him by saying:

"So one would be restricting things maybe on a kids phone so you can restrict some of the apps, because sometimes when kids aren't using their brain they could turn something on and someone could end up following them everywhere. This way the parent could see that and tell them to delete it" -P17

However, P22 who is also a father to a 2-year-old girl said that he didn't want to control it,

"So one of the parts that I have an idea for thinking about my daughter, I know that I can't be 100% monitoring her, so one of the things that I would like to know when she is using a smart phone is the kind of pictures that she is receiving or sharing because for now all the sex and photo sharing so I would like to have a section or an alert when she receives or she sends photos, so I can talk to her and ask her why she is sharing it. I don't want to stop it. I don't want to control her." -P22

This suggests that an activity feed can promote oversight for those that would like to guard close family members, such as parents and children from unsafe decisions. However, updates or oversight of others, such as strangers or friends, was an unwanted feature.

5.2.7 Non-Community Features: While the features discussed above promoted the community members to collaborate and advise each other, participants also designed certain features which did not require community member's participation or user-initiated commands. For example, ten out of 13 groups wanted the app to act as a watchdog and designed an app scanner to intercept their other apps and inform them of what was going on with their phones. P1 was one such individual who thought of this idea saying

"Any time you download any app it will track it and immediately, you know, scan it and make sure that nothing is violated based on the criteria we have on the privacy app." -P1

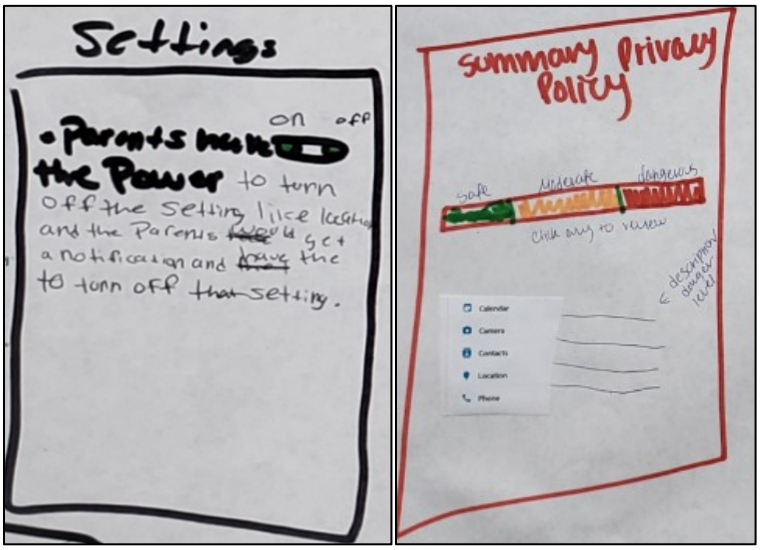

Fig. 7. Parental monitoring for activity feed (left, Group 3) and App Scanner, a non-community feature (right, Group 1)

P1 further said that the app should scan the phone like an antivirus program which can scan a given mobile app and give a threat assessment for each permission of that app in the form of a threat assessment bar. The permission will be grouped in three categories – safe (green), moderate (yellow) and dangerous (red) as shown in Figure 7 (right). Tapping on any of these three sections of the bar will list all the permissions that constitute elements of the tapped category. Although this idea may not be the most practical in practice, it does show how desperately participants wish to have a way to be more aware of what is going on with their phones in order to best act upon this information.

Participants were also concerned about apps invading their personal information, especially location, in the background when they are not using the app. To resolve this, 6 groups (G2, G4, G7, G8, G9, G11) designed a feature called privacy breach alerts which will notify the users if any app is using a resource without their knowledge. For example, if an app is accessing a user's location when they are not actively using the app, they would receive a notification about this breach. Group 9 (participant 21) resolved the similar problem in a different way. He proposed a unique feature called Location Timer where users can set a timer for how long they would like to

allow an app to access their location. After the time has passed, the location access to that app would be automatically turned off.

As previously mentioned, participants desired that app makers should be more transparent with their privacy information in order for individuals to make more informed and therefore smarter decisions about their mobile security. For instance, 6 groups (G1, G6, G7, G8, G9, G13) suggested that there should be a simplified version of privacy agreements provided by the app which summarizes the basic information like how the app would use user's personal data in a very easy to understand language, free of technical jargon.

"Yes, more information right at that point. I don't want to read ten pages before they even need anything. I want to see "can we use your location" and then there's a brief description right underneath that." -P15

Therefore, these features also suggest how participants delegated certain tasks to automation in order to passively help their community.

5.3 Trust as an Emergent Theme

When discussing the concepts of community, transparency, awareness, and individual participation in relation to designing an app for community oversight, trust was a theme that kept emerging during our interviews. While analyzing the data, we uncovered some disconnects between what we perceived for our model and participants' responses. We observed that participants desired transparency from not only app developers, but also the community members, strangers who are providing app reviews, and ratings. This need for transparent information suggested that trust is an important factor in utilizing provided guidance for decisions. In fact, the range of features participants explored, including the features that did not involve community involvement, indicate that users strongly desire trustworthy information to help them understand and make decisions regarding privacy on their mobile phones. While participants appreciated having information from strangers, they would most likely trust their known social connections more.

"I think because I have such a tight knit circle anybody within my circle, I would trust what they would say" -P11

Participants indicated they would certainly trust their close community members. However, community members may not provide enough information to help them, and thus information from strangers was desired. Yet, many indicated that trusting strangers was challenging and suggested ways to increase that trust. For example, in response to our question of who he would trust reviews from, participant 14 (Group 6) said that he would like if people who are providing a review give proof of why they are saying such thing,

"I would like proof, but yeah if they could back it up that way you could go and see it and verify it." -P14

Similarly, all the groups said that they would like to see the qualifications of the expert users. They said that having such information would help them feel more secure about following their advice. Participant 13 (group 6) said that expert users should be from companies like Norton, antivirus software by Symantec [77], who are well known for providing security, and are a perceived to be a reputable and trustworthy source. Participants also suggested being able to indicate their trust by having an option to validate user reviews through upvotes and downvotes in order to make sure that the review is authentic and correct. A final paradox that participants presented through our discussions is that while participants indicated that they were less trusting of anonymous reviews and comments, they also indicated that they would only be comfortable leaving comments publicly if they were anonymous. This leads to a remaining question as to how

to provide users with information that is both sufficiently useful and trustworthy to help them make decisions. We discuss this paradox and others presented in our results in the discussion and consider next steps in our design process.

6 DISCUSSION

In this section, we discuss our findings as they relate to participants perspectives of co-managing privacy and security. We then describe how results relate to our model and how we have extended our model considering new elements raised by participants. Lastly, we reflect upon limitations of our study and future work.

6.1 Revisiting the Model of Community Oversight (RQ1)

A novel contribution of our research was that we developed a theoretically driven model of community oversight (Figure 1). Then, we interrogated this model, revised, and extended it based on insights from our participatory design sessions. We present our updated model of community oversight in Figure 8. We made three major changes to this model: 1) Individual participation was divided into active and passive oversight and information sharing, 2) Trust was added as a foundational component of community oversight, and 3) We updated the callouts on the right-hand side of the model with the empirical findings from our participatory design sessions. We discuss some of the major insights from our study in more detail below.

One of the key lessons learned was that participants implicitly envisioned their community as their close-knit circles of family and friends, and sometimes, co-workers. Yet, paradoxically, participants broadened their definition of community when designing the app to a type of "social media" that included anyone willing to use the app to share relevant privacy and security information with others. This was often because they felt the needed expertise did not exist within their smaller social networks. While opening community to others, including strangers, offered them wider breadth of information, participants were also keenly aware of the negative trade-off between getting more information versus being able to trust the quality of the information they were given. This dilemma is reminiscent of the fake news phenomenon plaguing most social media platforms [3,65]. As a result, some groups tried to negotiate this tension by envisioning a

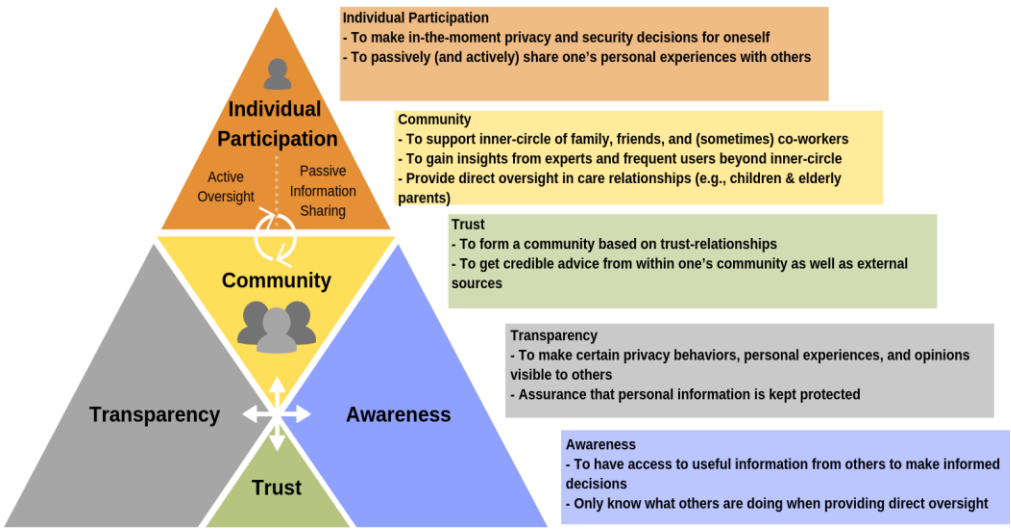

Fig. 8. Extended Model of Community Oversight

public/private feature to filter information based on whether someone was part of their community or an outsider of the community. One of the main things we observed from our participatory design exercise was that our participants were primarily motivated to help only their close family and friends with privacy and security decisions, not anyone else. They were most motivated to help when oversight involved a care-based relationship, such as parents looking after children, or adult children looking after elderly parents. This was evident from the features they designed to promote passive participation as compared to active participation and their rationale to support this during design discussion. Otherwise, they did not see this app as something they would use all the time, unless they were trying to decide about their own mobile app privacy and security. In general, individual participation needed to be lightweight and, in many cases, supported through automated features that did the work for them.

Similarly, participants were hesitant to make certain information visible within their communities, such as what apps they had installed on their smartphone. Instead, they were more willing to share innocuous information, such as reviews and ratings. This surfaced an important tension between transparency to the community and personal privacy. Participants did not want their privacy violated by their community in order to protect their privacy and security. Awareness was also characterized by asymmetry; individuals wanted to be made aware of relevant and trustworthy information when making decisions, but they did want to be made aware of when other community members were making privacy and security decisions. This was evidenced by the lack of interest in the Activity Feed, where individual actions were shared with the community. Finally, it became clear that trust was a critical mechanism for community oversight that was overlooked in our original model. As discussed in section 5.3, participants struggled the desire to keep their community exclusive to people they knew and trusted, but also wanted to benefit from expertise outside of these close-knit networks. Therefore, our revised model of community oversight highlights how participants refined the idea of community collaboration, and the kinds of participation they envisioned with various community members.,. We summarize how they designed for these tensions, as well as present design recommendations based on these findings in the sections that follow.

6.2 Translating Community Oversight into Useful App Features (RQ2)

Our participants gave us deeper insight into the types of features that they would value in a community oversight app for making digital privacy and security decisions. First, participants wanted high-quality, relevant, trusted, and aggregate information in the moment when they were trying to make a privacy and security decision. This was indicative in the review and ratings features (e.g., Discover, app reviews, and ratings), as well as the information sharing features (e.g., reviews and news). However, participants generally did not like the idea of constant transparency of others' activities or viewing information sharing among the larger community of app members in the form of activity feeds, unless they were in a parental role that required a more active level of individual oversight. Participants did not want to be inundated with irrelevant information, nor did they want to have to invest time in evaluating the quality of information. Also, they were willing to provide lightweight passive assistance to others (particularly their family and friends) through app ratings or sharing relevant news articles, but they did not see themselves doing this on an everyday basis. Generally, participants were too busy or inwardly focused to invest time in the active oversight of others, but conversely, they did recognize their own need for oversight in order to make better privacy and security decisions. This imbalance between the lack of motivation to help others versus the desire to get support will be the greatest challenge to making community oversight a feasible solution for digital privacy and security moving forward.

6.3 Design Implications for Overcoming Community Oversight Challenges (RQ3)

Our study shows the potential of using community oversight as a mechanism for helping people co-manage their digital privacy and security; however, it also uncovered significant challenges that must be overcome to do this. In this section, we provide some design-based recommendations based on the findings from our participatory design sessions.

6.3.1 Design Community as a Flexible Social Network: Based on our results, community could be re-envisioned from closed groups to reciprocal social networks of trusted connections. Participants were clear that they only wanted to help their inner circle, which included mostly family and friends. However, this social network structure should be flexible to allow for outside expertise. Therefore, a subscription model, like Twitter or Instagram, could be included where individuals could opt-in to unidirectional information provided by experts. Alternatively, outside expertise could be garnered through N levels of connection removed from an individual (drawing inspiration from Friendster [9]). This broadens the definition of community from a closed group (increasing the probability of expertise within the network) but maintains a higher level of personal connectedness rather than an unbounded open network. This solution serves to balance the tensions between expertise, trust, and community.

6.3.2 Leverage Automated Techniques to Foster Community: The mechanisms for promoting individual awareness through group-level transparency can be automated through this network structure. This would alleviate the need for active individual participation, while passively providing relevant and trusted information for making informed privacy and security decisions based on collective knowledge. Instead of participants having to self-initiate sharing, it would be done for them. Importantly, participants would need to be able to customize their privacy settings to ensure they are comfortable in their level of transparency within the community (e.g., ability to withhold information about certain apps installed on their phones).

6.3.3 Provide Support in the Context of Decision Making: Information should be aggregated and shared in the moment when a community member needs to make a privacy or security decision. Without a direct oversight relationship with another community member (e.g., a child or elderly parent), user do not care to know real-time information about the privacy and security decisions of other users. Instead, they only want to leverage this information when it is pertinent to their own decision-making processes. Therefore, features like the activity feed may be more suitable for active oversight and less useful for engagement with a community of like-minded strangers. However, features that do provide some details of an individual's decisions, on demand, may allow other individuals to provide occasional feedback.

6.3.4 Give Users Lightweight Mechanisms for Helping Each Other: To some extent, participants were willing to do passive information sharing, such as rating an app or sharing a relevant news article through direct message. While these types of interactions may be less frequent, giving users the ability to use lightweight passive sharing mechanisms may help foster a sense of community and caring about like-minded strangers.

6.3.5 Design for Trust and Information Quality: Even within a reciprocal social network, a way to assess the quality and reputation of advice is important. For instance, community members may designate some community members as expert users based on their contributions within the community or their known level of expertise (e.g., Aunt Anna is a cybersecurity expert). By allowing community members to self-organize around the strengths of individuals, this can

strengthen the community as a whole. Next, we will discuss some of the limitations of our research, challenges when designing for community oversight, and future areas of research.

6.4 Limitations and Future Work

We would like to highlight some of the limitations of our work that can be used to inform future research. First, since the concept of community oversight was so novel, we realized during our pilot studies that we needed to give participants a problem scenario to set the context, as well as some example features (e.g., Discover, Activity Feed, and Expert Users). Therefore, we provided participants with the "Movie Pass" scenario to help them transition into the study's goal of thinking about privacy and security for mobile applications. This scenario relates to entertainment apps, as opposed to other app types (e.g., banking, news, health monitoring, etc.), which may have influenced the features participants designed. Since the way that people think about privacy is often embedded in a particular social context [53], our future work will explore other contexts to understand community oversight for different types of apps, especially those that contain more sensitive information such as financial or health records.

Second, our sample was relatively small, and participants were recruited from a single geographic area in the Southeastern United States. We also did not specifically recruit from marginalized communities (e.g., LGBTQ+ [8], survivors of domestic violence [45] etc.), which are known to have unique privacy concerns in digital spaces. Therefore, our future work will include a larger sample of participants from more diverse backgrounds. One of our goals will be to move towards inclusive privacy and security design [55,69] for different communities of users. We plan to also study the unintended, and potentially harmful, negative impacts [10] of implementing a model of community oversight that includes individuals from marginalized communities. We will strive to ensure that our app cannot be used as a form of abusive control in relationships with significant power differentials (e.g., some domestic partnerships, children and parents, seniors, and adult children, etc.). For example, even though many of our participants liked the idea of using the app for parental monitoring, researchers within the SIGCHI community [30,47] have scrutinized this approach. For example, Ghosh et al. [30] found that parental control apps may be too restrictive, privacy invasive, and harm the trust-relationship between parents and their children, especially teens. Thus, this research should be considered when designing community oversight mechanisms for families.

Finally, an underlying assumption that we make in our research is that community can help improve an individuals' ability to make informed decisions about their digital privacy and security. While we base this claim on prior literature, this study does not empirically validate this claim. Our intent with this study was to create a novel model for community oversight and translate this model into a feature set for supporting collaborative privacy management. We plan to hold additional participatory design workshops to explore how community oversight is perceived in different types of communities, iterate on the design of our app, and continue to extend and explore our model of community oversight. Ultimately, our end goal is to design and implement a refined feature set within a "CO-oPS" mobile app and conduct longitudinal field studies to see whether and how users engage with the app and one another, as well as how this interaction influences their decision-making processes.

7 CONCLUSION

Our work began by building upon past literature to present a model of community oversight as a mechanism for helping people co-manage their digital privacy and security, relating concepts of transparency, awareness, and individual participation in supporting a community of users in

making privacy and security decisions. We explored this model in the domain of mobile app permissions through participatory design sessions and found that individuals saw potential gains from using a platform where they can discuss their privacy concerns with others. Although this model shows promise, participants in our study helped us to identify paradoxical relationships between designing useful mechanisms that make necessary information available and motivation to use such mechanisms on a regular basis.

These discussions helped to frame lessons learned about our model and features that support transparency, awareness, and individual participation. Desires for participants to have both sufficient and trustworthy information led to tensions surrounding the structure of a community and participation within the app. Thus, we revised our model to incorporate trust as well as the concept of active and passive participation. In addition, we need to further explore lightweight means of providing oversight that reflect the motivations of users to be helpful but not directly involved in others' decision-making. We will continue to design and explore these features, to investigate the potential of our model and how to provide support for social and community processes within technical solutions for privacy and security.

ACKNOWLEDGMENTS

We would like to thank the individuals who participated in our study. This research was supported by the U.S. National Science Foundation under grants CNS-1814068, CNS-1814110, and CNS-1814439. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

[1] Jarle Aarstad, Marcus Selart, and Sigurd Troye. 2011. Advice seeking network structures and the learning organization. *Problems and Perspectives in Management* 9, 2: 8.

[2] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services* (MobiSys '13), 97–110. https://doi.org/10.1145/2462456.2464460

[3] Hunt Allcott, Matthew Gentzkow, and Chuan Yu. 2019. *Trends in the Diffusion of Misinformation on Social Media.* National Bureau of Economic Research, Cambridge, MA. https://doi.org/10.3386/w25500

[4] Stephen J Andriole. 1992. *Rapid application prototyping: the storyboard approach to user requirements analysis.* QED Technical Publishing Group, Boston, Mass.

[5] Alastair R. Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. 2011. MockDroid: Trading Privacy for Application Functionality on Smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (HotMobile '11), 49–54. https://doi.org/10.1145/2184489.2184500

[6] John Carlo Bertot, Ursula Gorham, Paul T. Jaeger, Lindsay C. Sarin, and Heeyoon Choi. 2014. Big data, open government and e-government: Issues, policies and recommendations. *Information Polity* 19: 5–16. https://doi.org/10.3233/IP-140328

[7] John Carlo Bertot, Paul T. Jaeger, Sean Munson, and Tom Glaisyer. 2010. Social Media Technology and Government Transparency. *Computer* 43, 11: 53–59. https://doi.org/10.1109/MC.2010.325

[8] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 610–622. https://doi.org/10.1145/2858036.2858342

[9] Danah Michele Boyd. 2004. Friendster and Publicly Articulated Social Networking. In *CHI '04 Extended Abstracts on Human Factors in Computing Systems* (CHI EA '04), 1279–1282. https://doi.org/10.1145/985921.986043

[10] Brent Hecht, Lauren Wilcox, Jeffrey P. Bigham, Johannes Schöning, Ehsan Hoque, Jason Ernst, Yonatan Bisk, Luigi De Russis, Lana Yarosh, Bushra Anjum, Danish Contractor, and Cathy Wu. 2018. It's Time to Do Something: Mitigating the Negative Impacts of Computing Through a Change to the Peer Review Process. *ACM FCA*. Retrieved June 25, 2019 from https://acm-fca.org/2018/03/29/negativeimpacts/

[11] John M. Carroll and D. D. Reese. 2003. Community collective efficacy: structure and consequences of perceived capacities in the Blacksburg Electronic Village. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, 10 pp.-. https://doi.org/10.1109/HICSS.2003.1174585

[12] John M. Carroll, Patrick C. Shih, and Jessica Kropczynski. 2015. Community informatics as innovation in sociotechnical infrastructures. *J. Community Informatics* 11.

[13] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, 1. https://doi.org/10.1145/2335356.2335358

[14] Sunny Consolvo, Predrag Klasnja, David W. McDonald, and James A. Landay. 2009. Goal-setting Considerations for Persuasive Technologies That Encourage Physical Activity. In *Proceedings of the 4th International Conference on Persuasive Technology* (Persuasive '09), 8:1–8:8. https://doi.org/10.1145/1541948.1541960

[15] Sunny Consolvo, David W. McDonald, and James A. Landay. 2009. Theory-driven Design Strategies for Technologies That Support Behavior Change in Everyday Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09), 405–414. https://doi.org/10.1145/1518701.1518766

[16] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy in a Technology-filled World. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (SOUPS '14), 19–35. Retrieved June 25, 2019 from http://dl.acm.org/citation.cfm?id=3235838.3235841

[17] Rob Cross, Stephen P Borgatti, and Andrew Parker. 2001. Beyond answers: dimensions of the advice network. *Social Networks* 23, 3: 215–235. https://doi.org/10.1016/S0378-8733(01)00041-7

[18] Robert E. Crossler and France Bélanger. 2017. The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. https://doi.org/10.24251/hicss.2017.491

[19] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 143–157. Retrieved June 25, 2019 from https://www.usenix.org/conference/soups2014/proceedings/presentation/das

[20] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1416–1426. https://doi.org/10.1145/2675133.2675225

[21] Paul DiGioia and Paul Dourish. 2005. Social Navigation As a Model for Usable Security. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (SOUPS '05), 101–108. https://doi.org/10.1145/1073001.1073011

[22] Carl DiSalvo, Illah Nourbakhsh, David Holstius, Ayça Akin, and Marti Louw. 2008. The Neighborhood Networks Project: A Case Study of Critical Engagement and Creative Expression Through Participatory Design. In *Proceedings of the Tenth Anniversary Conference on Participatory Design 2008* (PDC '08), 41–50. Retrieved June 19, 2019 from http://dl.acm.org/citation.cfm?id=1795234.1795241

[23] Carl DiSalvo and Andrew Clement and Volkmar Pipek. 2012. Communities: Participatory Design for, with and by communities. *Communities: Participatory Design for, with and by communities Routledge International Handbook of Participatory Design, edited by Jesper Simonsen and Toni Robertson, Routledge, pp. 182–210.* https://doi.org/10.4324/9780203108543-15

[24] Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the Wild: User Strategies for Managing Security As an Everyday, Practical Problem. *Personal Ubiquitous Comput.* 8, 6: 391–401. https://doi.org/10.1007/s00779-004-0308-5

[25] Mica R. Endsley. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors* 37, 1: 32–64. https://doi.org/10.1518/001872095779049543

[26] Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods* 5, 1: 80–92. https://doi.org/10.1177/160940690600500107

[27] Leon Festinger. 1954. A Theory of Social Comparison Processes. *Human Relations* 7, 2: 117–140. https://doi.org/10.1177/001872675400700202

[28] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or Do Not, There is No Try: User Engagement May Not Improve Security Outcomes. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security* (SOUPS'16), 97–111. Retrieved July 24, 2018 from http://dl.acm.org/citation.cfm?id=3235895.3235904

[29] James Garofalo and Maureen McLeod. 1989. The Structure and Operations of Neighborhood Watch Programs in the United States. *Crime & Delinquency* 35, 3: 326–344. https://doi.org/10.1177/0011128789035003002

[30] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say About Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 124:1–124:14. https://doi.org/10.1145/3173574.3173698

[31] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela J. Wisniewski. 2018. A Matter of Control or Safety?: Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–14. https://doi.org/10.1145/3173574.3173768

[32] Peter Gilbert, Byung-Gon Chun, Landon P. Cox, and Jaeyeon Jung. 2011. Vision: automated security validation of mobile apps at app markets. In *Proceedings of the second international workshop on Mobile cloud computing and services - MCS '11*, 21. https://doi.org/10.1145/1999732.1999740

[33] Jeremy Goecks, W. Keith Edwards, and Elizabeth D. Mynatt. 2009. Challenges in Supporting End-user Privacy and Security Management with Social Navigation. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (SOUPS '09), 5:1–5:12. https://doi.org/10.1145/1572532.1572539

[34] Jürgen Habermas. 1984. *The theory of communicative action*. Beacon Press, Boston.

[35] Keith Hampton and Barry Wellman. 2003. Neighboring in Netville: How the Internet Supports Community and Social Capital in a Wired Suburb. *City and Community* 2, 4: 277–311. https://doi.org/10.1046/j.1535-6841.2003.00057.x

[36] Katy R. Holloway, Trevor H. Bennett, and David P. Farrington. 2008. Does Neighborhood Watch Reduce Crime? Retrieved June 25, 2019 from https://www.hsdl.org/?abstract&did=

[37] Victor W. Hwang and Greg Horowitt. 2012. *The Rainforest: The Secret to Building the Next Silicon Valley*. Regenwald, Los Altos Hills, Calif.

[38] Barbara A. Israel, Amy J. Schulz, Edith A. Parker, and Adam B. Becker. 1998. REVIEW OF COMMUNITY-BASED RESEARCH: Assessing Partnership Approaches to Improve Public Health. *Annual Review of Public Health* 19, 1: 173–202. https://doi.org/10.1146/annurev.publhealth.19.1.173

[39] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), 68–79.

[40] Holly Korda and Zena Itani. 2013. Harnessing social media for health promotion and behavior change. *Health Promotion Practice* 14, 1: 15–23. https://doi.org/10.1177/1524839911405850

[41] David Krackhardt and Jeffrey R. Hanson. 1993. Informal Networks: The Company Behind the Chart. *Harvard Business Review*. Retrieved July 24, 2018 from https://hbr.org/1993/07/informal-networks-the-company-behind-the-chart

[42] Rahim Kurwa. 2019. Building the Digitally Gated Community: The Case of Nextdoor. *Surveillance & Society* 17, 1/2: 111–117. https://doi.org/10.24908/ss.v17i1/2.12927

[43] Heather Richter Lipford and Mary Ellen Zurko. 2012. Someone to Watch over Me. In *Proceedings of the 2012 New Security Paradigms Workshop* (NSPW '12), 67–76. https://doi.org/10.1145/2413296.2413303

[44] Elizabeth J. Lyons, Zakkoyya H. Lewis, Brian G. Mayrsohn, and Jennifer L. Rowland. 2014. Behavior change techniques implemented in electronic lifestyle activity monitors: a systematic content analysis. *Journal of Medical Internet Research* 16, 8: e192. https://doi.org/10.2196/jmir.3469

[45] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17), 2189–2201. https://doi.org/10.1145/3025453.3025875

[46] K. R. McLeroy, D. Bibeau, A. Steckler, and K. Glanz. 1988. An ecological perspective on health promotion programs. *Health Education Quarterly* 15, 4: 351–377.

[47] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

[48] Andrew R. McNeill, Lynne Coventry, Jake Pywell, and Pam Briggs. 2017. Privacy Considerations when Designing Social Network Systems to Support Successful Ageing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17), 6425–6437. https://doi.org/10.1145/3025453.3025861

[49] Cheryl Merzel and Joanna D'Afflitti. 2003. Reconsidering Community-Based Health Promotion: Promise, Performance, and Potential. *American Journal of Public Health* 93, 4: 557–574. https://doi.org/10.2105/AJPH.93.4.557

[50] Darakhshan J. Mir, Yan Shvartzshnaider, and Mark Latonero. 2018. It Takes a Village: A Community Based Participatory Framework for Privacy Design. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 112–115. https://doi.org/10.1109/EuroSPW.2018.00022

[51] Michael J. Muller and Allison Druin. 2003. Participatory design: the third space in HCI. In *The Human-computer Interaction Handbook*, Julie A. Jacko and Andrew Sears (eds.). L. Erlbaum Associates Inc., Hillsdale, NJ, USA.

[52] Michael J. Muller and Sarah Kuhn. 1993. Participatory Design. *Commun. ACM* 36, 6: 24–28. https://doi.org/10.1145/153571.255960

[53] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[54] Sameer Patil, Xinru Page, and Alfred Kobsa. 2011. With a Little Help from My Friends: Can Social Navigation Inform Interpersonal Privacy Preferences? In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work* (CSCW '11), 391–394. https://doi.org/10.1145/1958824.1958885

[55] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us About Cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW: 139:1–139:24. https://doi.org/10.1145/3274408

[56] Anaïk Purenne and Grégoire Palierse. 2017. Towards Cities of Informers? Community-Based Surveillance in France and Canada. *Surveillance & Society* 15, 1: 79–93. https://doi.org/10.24908/ss.v15i1.5619

[57] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1: 121–144. https://doi.org/10.1093/cybsec/tyv008

[58] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12), 6:1–6:17. https://doi.org/10.1145/2335356.2335364

[59] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*, 272–288. https://doi.org/10.1109/SP.2016.24

[60] DENNIS P. ROSENBAUM. 1987. The Theory and Research Behind Neighborhood Watch: Is it a Sound Fear and Crime Reduction Strategy? *Crime & Delinquency* 33, 1: 103–134. https://doi.org/10.1177/0011128787033001007

[61] Mary Beth Rosson and John M. Carroll. 2003. The Human-computer Interaction Handbook. In Julie A. Jacko and Andrew Sears (eds.). L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 1032–1050. Retrieved November 8, 2018 from http://dl.acm.org/citation.cfm?id=772072.772137

[62] Robert J. Sampson, Jeffrey D. Morenoff, and Felton Earls. 1999. Beyond Social Capital: Spatial Dynamics of Collective Efficacy for Children. *American Sociological Review* 64, 5: 633–660. https://doi.org/10.2307/2657367

[63] Robert J. Sampson, Stephen W. Raudenbush, and Felton Earls. 1997. Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. *Science* 277, 5328: 918–924. https://doi.org/10.1126/science.277.5328.918

[64] Stephen Schneider. 2007. *Refocusing Crime Prevention: Collective Action and the Quest for Community.* University of Toronto Press. Retrieved March 10, 2019 from https://www.jstor.org/stable/10.3138/j.ctt2tv2h6

[65] Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Kaicheng Yang, Alessandro Flammini, and Filippo Menczer. 2018. The spread of low-credibility content by social bots. *Nature Communications* 9, 1. https://doi.org/10.1038/s41467-018-06930-7

[66] Wesley G. Skogan. 1989. Communities, Crime, and Neighborhood Organization. *Crime & Delinquency* 35, 3: 437–457. https://doi.org/10.1177/0011128789035003008

[67] Clay Spinuzzi. 2005. The methodology of participatory design. *Technical Communication*: 163–174.

[68] Beti Thompson, Gloria Coronado, Shedra A. Snipes, and Klaus Puschel. 2003. Methodologic Advances and Ongoing Challenges in Designing Community-Based Health Promotion Programs. *Annual Review of Public Health* 24, 1: 315–340. https://doi.org/10.1146/annurev.publhealth.24.100901.140819

[69] Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop* (NSPW 2017), 122–130. https://doi.org/10.1145/3171533.3171538

[70] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy Nudges for Social Media: An Exploratory Facebook Study. In *Proceedings of the 22Nd International Conference on World Wide Web Companion* (WWW '13 Companion), 763–770. Retrieved June 12, 2015 from http://dl.acm.org/citation.cfm?id=2487788.2488038

[71] Barry Wellman. 2005. Community: from neighborhood to network. *Communications of the ACM* 48, 10: 53. https://doi.org/10.1145/1089107.1089137

[72] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety? In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17*, 51–69. https://doi.org/10.1145/2998181.2998352

[73] Catherine G. Wolf and John Karat. 1997. Capturing What is Needed in Multi-user System Design: Observations from the Design of Three Healthcare Systems. In *Proceedings of the 2nd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques* (DIS '97), 405–415. https://doi.org/10.1145/263552.263656

[74] Hengshu Zhu, Hui Xiong, Yong Ge, and Enhong Chen. 2014. Mobile app recommendations with security and privacy awareness. In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '14*, 951–960. https://doi.org/10.1145/2623330.2623705

[75] Demographics of Mobile Device Ownership and Adoption in the United States. Retrieved September 25, 2018 from http://www.pewinternet.org/fact-sheet/mobile/

[76] What is a mobile threat? Retrieved June 20, 2019 from https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat
[77] Official Site | Norton™ - Antivirus & Cybersecurity Software. Retrieved April 4, 2019 from https://us.norton.com/

Received April 2019; revised June 2019; accepted August 2019.